80

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/863,384	05/24/2001	Shingo Yamaguchi	203223US-28	1503

22850 7590 05/31/2005

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 05/31/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/863,384	YAMAGUCHI, SHINGO	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 March 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *41-80* is/are pending in the application.

4a) Of the above claim(s) *1-40* is/are ~~withdrawn from consideration.~~ canceled.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *41-80* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ ~~Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)~~ Paper No(s)/Mail Date *5/24/01 & 8/9/01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ ~~Notice of Informal Patent Application (PTO-152)~~
6) ☐ Other: _____.

5-0-21

DETAILED ACTION

1. Applicant has amended by adding new claims 41-80.

Claims 1-40 have been cancelled.

2. Claims 41-42, 44, 46-62, 64, and 66--80 have been examined and are rejected under 35 U.S.C. 102(e).

Claims 43, 45, 63, and 65 have been examined and are rejected under 35 U.S.C. 103(a).

This is a Final rejection necessitated by new grounds of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 41-42, 44, 46-62, 64, and 66--80 are rejected under 35 U.S.C. 102(e) as being anticipated by Flint, et al. (US 6,453,419).

As per claim 41:

Flint, et al. discusses a method of controlling a network, comprising the steps of:

establishing a computer network connection between a computer **[COL.2, lines 30-42]** and an intermediate device which has network resources connected thereto; **[COL.3, lines 36-39]**

determining a level of security of the computer network connection **[COL.3, line 48 – COL.4, line 1]** based on determining a communication protocol of the computer network connection to connect the computing device to the intermediate device; and **[COL.11, lines 58-59]**

controlling a level of access of the computing device to the network resources **[COL.4, lines 28-43]** using the level of security of the computer network connection which that has been determined. **[COL.5, lines 1-4 and COL.6, lines 7-10]**

As per claim 42: **See COL.3, lines 33-39;** discusses establishing a wireless computer network connection.

As per claim 44: **See COL.3, line 48 – COL.4, line 1 and Col. 11, lines 58-59;** discusses determining a level of security, the determining the communication protocol determines whether the computer network connection is encrypted.

As per claim 46: **See COL.3, lines 3-63;** discusses allowing the computer to access a file server which is one of the network resources, only when the step of determining the level of security determines that the computer network connection is encrypted.

As per claim 47: **See COL.3, lines 45-46;** discusses allowing the computer to

access the Internet which is one of the network resources, regardless of whether the computer network connection is encrypted.

As per claim 48: **See COL.6, line 9;** discusses allowing the computer to access an email server which is one of the network resources, regardless of whether the computer network connection is encrypted.

As per claim 49: **See COL.3, lines 15-25 and 54-57;** discusses allowing the computer to access an email server which is one of the network resources, only when the computer network connection is encrypted.

As per claim 50: **See COL.3, lines 47-53;** discusses the step of determining is performed by the intermediate device, and said controlling is performed by the intermediate device.

As per claim 51: **See COL.2, lines 15-20;** discusses the step of determining is performed by the intermediate device which is a router.

As per claim 52: **See COL.2, lines 15-20 and COL.3, lines 48-53;** discusses the step of controlling is performed by the intermediate device which is a router having a firewall operation.

As per claim 53: **See COL.2, lines 15-20 and COL.3, lines 33-39;** discusses the step of establishing is performed using the intermediate device which is a router which establishes a wireless connection to the computer.

As per claim 54: **See COL.3, lines 15-26 and COL.6, lines 22-24;** discusses the step of determining is performed by a server running a network operating system, the

server being different from the intermediate device, and the step of controlling is performed by the server running the network operating system.

As per claim 55: **See COL.3, lines 54-60;** discusses the step of determining is performed by the server which is running a network directory service.

As per claim 56: **See COL.2, lines 15-20;** discusses the step of establishing is performed by a bridge connected to the computer through the computer network connection.

As per claim 57: **See COL.2, lines 15-20 and COL.3, lines 33-39;** discusses the step of establishing is performed by the bridge connected to the computer through the computer network connection which is a wireless network connection.

As per claim 58: **See COL.3, lines 3-9 and 48-50;** discusses the level of access by a stand-alone firewall device which is connected between the intermediate device and the network resources.

As per claim 59: **See COL.11, lines 58-60;** discusses determining the level of security using the intermediate device.

As per claim 60: **See COL.3, lines 33-39;** establishing the computer network connection as a wireless connection using the intermediate device.

As per claim 61:

Flint, et al. discusses a method of controlling a network, comprising the steps of:

means for establishing a computer network connection between a computer **[COL.2, lines 30-42]** and an intermediate device which has network resources connected thereto; **[COL.3, lines 36-39]**

means for determining a level of security of the computer network connection **[COL.3, line 48 – COL.4, line 1]** based on determining a communication protocol of the computer network connection to connect the computing device to the intermediate device; and **[COL.11, lines 58-59]**

means for controlling a level of access of the computing device to the network resources **[COL.4, lines 28-43]** using the level of security of the computer network connection which that has been determined. **[COL.5, lines 1-4 and COL.6, lines 7-10]**

As per claim 62: **See COL.3, lines 33-39;** discusses means for establishing a wireless computer network connection.

As per claim 64: **See COL.3, line 48 – COL.4, line 1 and 11, lines 58-59;** discusses means for determining whether the computer network connection is encrypted.

As per claim 66: **See COL.3, lines 3-63;** discussing means for allowing the computer to access a file server which is one of the network resources, only when the means for determining the level of security determines that the computer network connection is encrypted.

As per claim 67: **See COL.3, lines 45-46;** discusses means for allowing the computer to access the Internet which is one of the network resources, regardless of whether the computer network connection is encrypted.

As per claim 68: **See COL.6, line 9;** discusses means for allowing the computer to access an email server which is one of the network resources, regardless of whether the computer network connection is encrypted.

As per claim 69: **See COL., lines ;** discusses means for allowing the computer to

access an email server which is one of the network resources, only when the computer network connection is encrypted.

As per claim 70: **See COL.3, lines 15-25 and 54-57;** discusses the means for determining is the intermediate device, and the means for controlling is the intermediate device.

As per claim 71: **See COL.2, lines 15-20;** discusses the means for determining is the intermediate device which is a router.

As per claim 72: **See COL.2, lines 15-20 and COL.3, lines 48-53;** discusses the means for controlling is the intermediate device which is a router having a firewall operation.

As per claim 73: **See COL.2, lines 15-20 and COL.3, lines 33-39;** discusses the means for establishing is the intermediate device which is a router which establishes a wireless connection to the computer.

As per claim 74: **See COL.3, lines 15-26 and COL.6, lines 22-24;** discusses the means for determining is a server running a network operating system, the server being different from the intermediate device, and the means for controlling is the server running the network operating system.

As per claim 75: **See COL.3, lines 54-60;** discusses the means for determining is the server which is running a network directory service.

As per claim 76: **See COL.2, lines 15-20;** discusses the means for establishing is a bridge connected to the computer through the computer network connection.

As per claim 77: **See COL.2, lines 15-20 and COL.3, lines 33-39;** discusses the

means for establishing is the bridge connected to the computer through the computer network connection which is a wireless network connection.

As per claim 78: See COL.3, lines 3-9 and 48-50; discusses a stand-alone firewall device which is connected between the intermediate device and the network resources.

As per claim 79: See COL.11, lines 58-60discusses means for determining the level of security using the intermediate device.

As per claim 80: See COL.3, lines 33-39; discusses means for establishing the computer network connection as a wireless connection using the intermediate device.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 43, 45, 63, and 65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flint, et al. (US 6,453,419) and further in view of Official Notice.

As per claim 43:

Flint discusses establishing computer network connection between a computing device and a firewall that has network resources connected thereto wherein the firewall controls communications between networks and the Virtual Private Network which can be a wireless network connection **[COL.3, lines 17-39]**. However, Flint fails to implicitly include the IEEE 802.11b standard and takes official notice of such standard.

It is well known in the art at the time of the invention, an IEEE 802.11b standard allows computers and other devices to communicate over a wireless network.

As per claim 45:

Flint discusses establishing computer network connection between a computing device and a firewall that has network resources connected thereto wherein the firewall controls communications between networks and the Virtual Private Network which can be a wireless network connection **[COL.3, lines 17-39]**. However, Flint fails to imply the Wired Equivalent Privacy ("WEP") encryption method.

It is well known in the art at the time of the invention that Wired Equivalent Privacy ("WEP") encryption is used in a IEEE 802.11b standard environment because WEP encryption ensures data is not transmitted in the clear over the wireless network that WEP enables encryption between the client and the wireless access point.

As per claim 63:

Flint discusses establishing computer network connection between a computing device and a firewall that has network resources connected thereto wherein the firewall controls communications between networks and the Virtual Private Network which can

be a wireless network connection **[COL.3, lines 17-39]**. However, Flint fails to implicitly include the IEEE 802.11b standard and takes official notice of such standard.

It is well known in the art at the time of the invention, an IEEE 802.11b standard allows computers and other devices to communicate over a wireless network.

As per claim 65:

Flint discusses establishing computer network connection between a computing device and a firewall that has network resources connected thereto wherein the firewall controls communications between networks and the Virtual Private Network which can be a wireless network connection **[COL.3, lines 17-39]**. However, Flint fails to imply the Wired Equivalent Privacy ("WEP") encryption method.

It is well known in the art at the time of the invention that Wired Equivalent Privacy ("WEP") encryption is used in a IEEE 802.11b standard environment because WEP encryption ensures data is not transmitted in the clear over the wireless network that WEP enables encryption between the client and the wireless access point.

Response to Arguments

5. Applicant's arguments with respect to claims 41-80 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax

phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa

KIM V.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100